JOURNAL OF ALGEBRA 8, 393-414 (1968)

On Loops of Odd Order II

GEORGE GLAUBERMAN

University of Chicago, Chicago, Illinois

Communicated by R. H. Bruck

Received February 2, 1967

1. INTRODUCTION AND NOTATION

Let H be a finite (multiplicative) Moufang loop of odd order. One may show (Lemma 1) that each element x of H has a unique square root $x^{1/2}$ and that with respect to the operation $\circ$, given by $x \circ y = x^{1/2}yx^{1/2}$, H forms a power-associative loop $H(\frac{1}{2})$. This loop satisfies the identical relations

$$x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z, \qquad (x \circ y)^{-1} = x^{-1} \circ y^{-1}, \qquad (1)$$

where x^{-1} denotes the inverse of x under $\circ$. In [5], we studied loops of this type and verified analogues of some well-known results of Sylow, Lagrange, and P. Hall on finite groups. In this paper we use these analogues to prove the corresponding results for Moufang loops of odd order.

We also stated in [5] a group-theoretical conjecture equivalent to the proposition that every finite B-loop is solvable. Recently we proved this conjecture [6]. In Section 6, we therefore show that all finite B-loops and also all finite Moufang loops are solvable. Since the class of Moufang loops includes the class of groups, the latter result generalizes the theorem of Feit and Thompson [4] on groups of odd order. However, the results of Section 6 require the Feit-Thompson theorem. Therefore, we have thought it more interesting to place Section 6 at the end of the paper, although its contens are idependent of the main results of the preceding sections and could be used to shorten some of the proofs.

Most of our results are not valid for Moufang loops of even order. These loops need not be solvable, e.g., the finite simple non-cyclic groups, and the finite simple non-associative Moufang loops discovered by Paige [9]. Although Moufang loops of odd order possess Sylow subloops, Paige's loop of order 120 contains no element of order 5. However, some analogues of our results are obtained in the following paper [7].

We adopt the following notation. Suppose x is an arbitrary element of an arbitrary set S. If σ and μ are permutations of S, write $[x]\,\sigma$ or x^σ for the

image of x under σ and let $[x]\,(\sigma\mu) = [[x]\,\sigma]\,\mu$. If T is a subset of S, let $[T]\,\sigma$ be the set $\{[x]\,\sigma : x \in T\}$. We say that σ *fixes* an element or subset T of S if $[T]\,\sigma = T$. In general, we will employ the notation of [2]. We define permutations $R(x)$, $L(x)$, $T(x)$, and $P(x)$ by $[y]\,R(x) = yx$, $[y]\,L(x) = xy$, $T(x) = L(x)^{-1}\,R(x)$, $P(x) = R(x)\,L(x)$. Note that $[y]\,P(x) = xyx = x^2 \circ y$.

In any Moufang loop G we shall let $\langle x, y, z, \ldots\rangle$ be the subloop of G generated by the elements or sets x, y, z,... . In particular, for $G = H$ this means the subloop of H generated under the original (Moufang) operation of H, which does not necessarily coincide with the subloop of H generated by x, y, z,... under $\circ$. Let M_H, the *multiplicative group* of H, be the group of permutations $\langle R(x), L(x) : x \in H\rangle$. Then I_H, the group of *inner mappings* of H, is $\langle T(x), R(x)\,R(y)\,R(xy)^{-1}, L(x)\,L(y)\,L(yx)^{-1} : x, y \in H\rangle$. Let K be any subloop of H. We let $R_K = \langle R(x) : x \in K\rangle$, $L_K = \langle L(x) : x \in K\rangle$, $T_K = \langle T(x) : x \in K\rangle$, $P_K = \langle P(x) : x \in K\rangle$,

$$M_K = \langle R_K, L_K\rangle, \qquad \text{and} \qquad I_K = I_H \cap M_K .$$

Let $P(K)$ be the set $\{P(x) : x \in K\}$.

We denote the identity element of H by 1. If $x \in H$ we let x^0 be 1. For $x, y, z \in H$ we let (x, y, z) be the *associator* of x, y, and z, given by $(x, y, z) = (x(yz))^{-1}\,((xy)\,z)$. For non-empty subsets A, B, C of H we let

$$(A, B, C) = \langle (x, y, z) : x \in A, y \in B, z \in C\rangle.$$

In any Moufang loop G we let $Z(G)$ be the center of G.

Throughout this paper we assume H is an arbitrary finite (multiplicative) Moufang loop of odd order. We shall refer to [5] as I and to result x of [5] as result I.x.

2. Some Basic Properties

Lemma 1. (a) *Let $x \in H$. The order of x divides the order of H. Let x have order $2n - 1$ and let $x^{1/2} = x^n$. If $y \in H$, then $y^2 = x$ if and only if $y = x^{1/2}$.*

(b) *$H(\frac{1}{2})$ is a power-associative loop which satisfies* (1)*, and 1 is its identity element.*

(c) *Let $x \in H$. For any integer m, the power x^m is the same whether computed in H or in $H(\frac{1}{2})$. In particular, x has the same order under both operations, and $x^{1/2}$ and x^{-1} are the same in H as in $H(\frac{1}{2})$.*

(d) *Every nonempty subset of H which is closed under $\circ$ is a subloop of $H(\frac{1}{2})$.*

Proof. (a) The order of x divides the order of H because H is diassociative ([2], Theorem V.1.2, p. 92). Hence the order of x is odd, say, $2n-1$. Certainly $(x^{1/2})^2 = x^{2n} = x^{2n-1}x = x$. Suppose $y^2 = x$. Then $y^{4n-2} = x^{2n-1} = 1$. Since y has odd order, $y^{2n-1} = 1$. Hence

$$y = y^{2n} = (y^2)^n = x^n = x^{1/2}.$$

(b) This is part of Theorem VII.5.2, p. 121, of [2].

(c) The proof of Lemma I.5(ii) also applies here.

(d) This is Lemma I.4.

Let π be a set of primes. We say that a positive integer n is a *π-number* if every prime divisor of n lies in π. Let K be a finite power-associative loop; then K is a *π-loop* if the order of every element of K is a π-number. If $\pi = \{p\}$, a π-loop is also called a p-loop. We let $|S|$ be the number of elements of an arbitrary finite set S.

THEOREM 1. *Let π be a set of primes. Then H is a π-loop if and only if $|H|$ is a π-number.*

Proof. By Lemma 1(c), H is a π-loop if and only if $H(\frac{1}{2})$ is a π-loop. By Corollary 2 of Theorem I.9, $H(\frac{1}{2})$ is a π-loop if and only if $|H|$ is a π-number.

THEOREM 2. *Let K be a subloop of H. Then K forms a subloop of $H(\frac{1}{2})$ and $|K|$ divides $|H|$.*

Proof. Let x and y be arbitrary elements of K. Since x has finite odd order, $x^{1/2}$ is a power of x and therefore lies in K. Hence $x \circ y = x^{1/2}yx^{1/2} \in K$. By Lemma 1(d), K is a subloop of $H(\frac{1}{2})$. By Corollary 4 of Theorem I.9, $|K|$ divides $|H|$.

LEMMA 2. (a) *The mapping $x \to P(x)$ is a one-to-one correspondence of H onto $P(H)$.*

(b) *Define an operation $\circ'$ on $P(H)$ by $P(x) \circ' P(y) = P(x^{1/2})\,P(y)\,P(x^{1/2})$. Then $P(x) \circ' P(x) = P(x)^2$ and $P(x \circ y) = P(x) \circ' P(y)$ for all $x, y \in H$.*

(c) *If J is a subgroup of M_H, then $J \cap P(H)$ is a subloop of $P(H)$ with respect to $\circ'$.*

Proof. (a) Suppose $P(x) = P(y)$. Then

$$x^2 = x1x = [1]\,P(x) = [1]\,P(y) = y^2.$$

Hence $y = (x^2)^{1/2} = x$.

(b) By (a), the operation $\circ'$ is well-defined. Let $z \in H$. Then

$$[z]\, P(x) \circ' P(y) = [z]\, P(x^{1/2})\, P(y)\, P(x^{1/2}) = x \circ (y^2 \circ (x \circ z))$$

$$= (x \circ (y^2 \circ x)) \circ z$$

by (1). But $x \circ (y^2 \circ x) = x^{1/2}yxyx^{1/2} = (x^{1/2}yx^{1/2})^2 = (x \circ y)^2$. Hence $[z]\, P(x) \circ' P(y) = (x \circ y)^2 \circ z = [z]\, P(x \circ y)$. Thus $P(x) \circ' P(y) = P(x \circ y)$. In particular, $P(x) \circ' P(x) = P(x \circ x) = P(x^2) = P(x)^2$.

(c) Let $P(x)$, $P(y) \in J \cap P(H)$. Let x have order $2n - 1$. Then $P(x^{1/2}) = P(x^n) = P(x)^n \in J$. Hence

$$P(x) \circ' P(y) = P(x^{1/2})\, P(y)\, P(x^{1/2}) \in J \cap P(H).$$

Now we apply (a), (b), and Lemma 1(d).

As usual, we say that a triple (U, V, W) of permutations of H is an *autotopism* of H if $([x]\, U)\,([y]\, V) = [xy]\, W$ for all $x, y \in H$. An element z lies in the *nucleus* of H if $(xy)\, z = x(yz)$, $(xz)\, y = x(zy)$, and $z(xy) = (zx)\, y$ for all $x, y \in H$. The nucleus forms a normal subloop of H ([2], Theorem VII. 2.1, p. 114) which we denote by Nuc (H).

LEMMA 3 ([2], pp. 112-114). *If $x \in H$, the triples $A(x)$ and $B(x)$ given by $(P(x), L(x)^{-1}, L(x))$ and $(R(x)^{-1}, P(x), R(x))$ respectively, are automorphisms of H. If $(1, V, W)$ is an autotopism of H, then $V = W = R(c)$ for some $c \in$ Nuc (H). Under the multiplication defined by*

$$(U, V, W)\,(U', V', W') = (UU', VV', WW'),$$

the autotopisms of H form a group.

LEMMA 4. *Let σ be an inner mapping of H.*

(a) *As a mapping on $H(\frac{1}{2})$, σ is an automorphism.*

(b) *The elements of H which are fixed by σ form a subloop of $H(\frac{1}{2})$.*

(c) *If $x \in H$, then $\sigma^{-1}P(x)\, \sigma = P(x^\sigma)$.*

(d) *Let K be any subloop of H. Then I_K normalizes $P(K)$, and P_K is a normal subgroup of M_K. Moreover, $M_K = T_K P_K = I_K P_K$.*

(e) $M_K = R_K P_K = L_K P_K$.

Proof. (a) This follows from [2], Lemma VII.3.2, p. 117, and Theorem VII.5.2, p. 121.

(b) Apply (a) and Lemma 1(d).

(c) Let $x, y \in H$. Then $[y]\, \sigma^{-1}P(x)\, \sigma = [y^{\sigma^{-1}}]\, P(x)\, \sigma = (x^2 \circ y^{\sigma^{-1}})^\sigma$. By (a), $(x^2 \circ y^{\sigma^{-1}})^\sigma = (x^2)^\sigma \circ (y^{\sigma^{-1}})^\sigma = (x^\sigma)^2 \circ y = [y]\, P(x^\sigma)$.

(d) Clearly I_K normalizes $P(K)$ by (c). Since

$$M_K = \langle R(x), L(x) : x \in K\rangle = \langle R(x^2), L(x^2) : x \in K\rangle$$
$$= \langle L(x)^{-1} R(x), L(x) R(x) : x \in K\rangle = \langle T_K , P_K\rangle \subseteq \langle I_K , P_K\rangle,$$

we see that M_K normalizes P_K and that $M_K = T_K P_K = I_K P_K$.

(e) Let $x \in K$. Then $R(x) = R(x)\,1$ and $L(x) = R(x^{-1})\,P(x)$. Thus $M_K = \langle R_K , P_K\rangle = R_K P_K$. Similarly, $M_K = \langle L_K , P_K\rangle = L_K P_K$.

We say that a loop K is *solvable* if there exists a series

$$K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_n = 1 \tag{2}$$

with the property that for $i = 1, 2,..., n$, K_i is a normal subloop of K_{i-1} and K_{i-1}/K_i is a commutative group.

THEOREM 3. *Let π be a set of primes and let K be a solvable π-subloop of H. Then $K(\frac{1}{2})$ is a solvable π-loop and M_K is a solvable π-group.*

Proof. By Theorem 2, K is a subloop of $H(\frac{1}{2})$ and $|K|$ is a π-number. By Lemma 1(c), $K(\frac{1}{2})$ is a π-loop. Now K has a series of the form (2). By using the same series, we see that $K(\frac{1}{2})$ is solvable. Take $\circ'$ as in Lemma 2; then $P(K)$ forms a loop under $\circ'$ which is isomorphic to $K(\frac{1}{2})$. Hence by Theorem I.6, P_K is a solvable π-group.

Let $g \in L_K$. We may write g as a product $g = L(x_1) L(x_2) \cdots L(x_r)$ for $x_1 , x_2 ,..., x_r \in K$. Let $h = P(x_1) P(x_2) \cdots P(x_r)$, $k = L(x_1)^{-1} L(x_2)^{-1} \cdots L(x_r)^{-1}$, and $A_0 = A(x_1) A(x_2) \cdots A(x_r)$ for $A(x)$ as defined in Lemma 3. Then $A_0 = (h, k, g)$. Let m be the order of h. Then

$$(A_0)^m = (h^m, k^m, g^m) = (1, k^m, g^m).$$

By Lemma 3, $g^m = R(c)$ for some $c \in \mathrm{Nuc}\,(H)$. Since each element of L_K maps K onto itself, $c = [1]\,R(c) \in K$. Let n be the order of c. Then $R(c)^n = R(c^n) = R(1) = 1$. Thus $g^{mn} = 1$. Since $h \in P_K$ and $c \in K$, m and n are π-numbers. Hence the order of g is a π-number. Thus L_K is a π-group.

Let d be the derived length of P_K and let $J = K \cap \mathrm{Nuc}\,(H)$. By considering commutators of the group $\langle A(x) : x \in K\rangle$ and using the method of the above paragraph, we see that $(L_K)^{(d)} \subseteq \langle R(c) : c \in J\rangle$. But it is easy to see that if $x, y \in J$, then $xy \in J$ and $R(x)\,R(y) = R(xy)$. Hence $(L_K)^{(d)}$ is isomorphic to a subgroup of J. Since $J \subseteq K$, J is solvable. Thus $(L_K)^{(d)}$, and hence L_K, are solvable.

Thus both L_K and P_K are solvable π-groups. By Lemma 4, M_K is a solvable π-group.

THEOREM 4. *If $|H|$ is a power of a prime, then H is centrally nilpotent.*

Proof. Suppose $|H|$ is a power of a prime p. By Theorem I.7, $H(\frac{1}{2})$ is centrally nilpotent. By Theorem I.6 and Lemma 2, P_H is a p-group. As in the second paragraph of the proof of Theorem 3, we see that L_H is a p-group. By Lemma 4(e), $M_H = L_H P_H$, which is a p-group. Therefore, H is centrally nilpotent ([2], Lemma VI.2.2, p. 98).

COROLLARY. *Every finite commutative Moufang loop (of even or odd order) is a direct product of an Abelian group of order relatively-prime to 3 and a commutative, centrally nilpotent 3-loop.*

Remark 1. This result is a special case of a theorem of R. H. Bruck ([2], pp. 130-131) that every finitely-generated commutative Moufang loop is centrally nilpotent. The author thanks Professor Bruck for suggesting the following proof, which replaces a more complicated one by the author.

Proof. Let K be a finite commutative Moufang loop. Let A be the set of all elements of K having order relatively prime to 3. If $x, y \in A$, then x and y generate a commutative group. Hence $x^{-1}, xy \in A$. Thus A is a subloop of K. Since inner mappings of K preserve orders of elements. A is a normal subloop of K. Similarly, those elements of K whose orders are (nonnegative) powers of 3 form a normal subloop B of K. Now $A \cap B = 1$. Since every element of K is a product of an element of A and an element of B, $K = AB$. So, $K = A \times B$.

Let $x \in A$. By Lemma VII.3.3, p. 117, of [2], every inner mapping of K is an automorphism. Since the inner mapping $y \to x^{-1}yx$, $y \in K$, has companion x^{-3}, we have $x^{-3} \in \mathrm{Nuc}\,(K)$. But the order of x is relatively prime to 3. Hence $x \in \mathrm{Nuc}\,(K)$. Thus $A \subseteq \mathrm{Nuc}\,(K)$, and A is a commutative group.

Since the nonidentity elements of B can be partitioned into disjoint pairs of the form $\{x, x^{-1}\}$, $|B|$ is odd. Therefore, our previous results apply to B. Since B is a 3-loop, $|B|$ is a power of 3, by Theorem 1. By Theorem 4, B is centrally nilpotent.

THEOREM 5. *The following conditions are equivalent:*

(a) *H is centrally nilpotent;*

(b) *for every prime p, those elements whose orders are (nonnegative) powers of p form a subloop of H;*

(c) *H is a direct product of p-loops for some primes p.*

Proof. Assume (a). Let $x, y \in H$. Then x and y generate a finite nilpotent group K. Now, K is a direct product of its Sylow subgroups. Therefore, if x and y lie in a Sylow subgroup of K, so do x^{-1} and xy. Therefore, H satisfies (b).

Assume (b). We will prove (c). For every prime p, let H_p be the subloop of H consisting of those elements whose orders are powers of p; since inner mappings preserve orders of elements, H_p is a normal subloop of H. Let π be the set of primes p for which $H_p \neq 1$.

We prove by induction that if $p_1, \ldots, p_n$ are distinct primes in π, then $H_{p_1} \cdots H_{p_n} = H_{p_1} \times \cdots \times H_{p_n}$. This is obvious for $n = 1$. Suppose it holds for $n = k$. Take $n = k + 1$. Let $K = H_{p_1} \cdots H_{p_k}$. Then $K = H_{p_1} \times \cdots \times H_{p_k}$. Therefore, K has no nonidentity elements whose order is a power of p_{k+1}. Thus K and $H_{p_{k+1}}$ are normal subloops of $KH_{p_{k+1}}$ that intersect in the identity loop. Hence $KH_{p_{k+1}} = K \times H_{p_{k+1}}$. So, by induction hypothesis,

$$H_{p_1} \cdots H_{p_k} H_{p_{k+1}} = KH_{p_{k+1}} = K \times H_{p_{k+1}} = H_{p_1} \times \cdots \times H_{p_k} \times H_{p_{k+1}}.$$

If $|H| = 1$, then (c) holds trivially. If $|H| > 1$, let $p_1, \ldots, p_n$ be the distinct primes in π. Then $H = H_{p_1} \cdots H_{p_n} = H_{p_1} \times \cdots \times H_{p_n}$. Thus H satisfies (c).

Assume (c). By Theorem 4, H is centrally nilpotent. This completes the proof of Theorem 5.

3. Automorphisms of M_H

Certain automorphisms of M_H are useful for discovering the structure of of H. Let a be the inverse mapping of H, i.e., let a be the permutation of H given by $[x]\, a = x^{-1}$, $x \in H$. If $x, y \in H$, then

$$[y]\, a^{-1}R(x)\, a = [y]\, aR(x)\, a = [y^{-1}]\, R(x)\, a = x^{-1}y = [y]\, L(x^{-1}).$$

Hence, $a^{-1}R(x)\, a = L(x^{-1})$. Similarly, $a^{-1}L(x)\, a = R(x^{-1})$. Thus a normalizes M_H. We let α be the automorphism of M_H defined by $g^\alpha = a^{-1}ga$.

Lemma 5 ([2], Lemma IV.1.2, p. 61). *Let $g \in M_H$. Then $g \in I_H$ if and only if $[1]\, g = 1$.*

Remark 2. One may observe in the following that parts (a) and (b) of Lemma 6 and all of Theorem 6 except part (c) hold for arbitrary Moufang loops; H need not have finite odd order.

Lemma 6. (a) *If $x \in H$, then $R(x)^\alpha = L(x)^{-1}$, $L(x)^\alpha = R(x)^{-1}$, and $P(x)^\alpha = P(x)^{-1}$.*

(b) *If $\sigma \in I_H$, then $\sigma^\alpha = \sigma$.*

(c) *Let $g \in M_H$. There exist unique elements $t \in I_H$ and $x \in H$ such that $g = tP(x)$. For these elements, $[1]\, g = x^2$ and $g^{-1}g^\alpha = P(x)^{-2}$.*

(d) *Let J be a subgroup of M_H that is fixed by α. Every element g of J has a unique representation of the form $tP(x)$ such that $t \in J \cap I_H$, $x \in H$ and $P(x) \in J$. Moreover, $|J| = |J \cap I_H|\,|J \cap P(H)|$.*

Proof. (a) This follows from easy computations.

(b) Let $\sigma \in I_H$ and $x \in H$. By Lemma 4(a),

$$[x]\,\sigma^\alpha = [x]\,a\sigma a = [x^{-1}]\,\sigma a = [(x^\sigma)^{-1}]\,a = x^\sigma = [x]\,\sigma.$$

(c) Let $x = ([1]\,g)^{1/2}$ and let $t = gP(x)^{-1}$. Then

$$[1]\,t = [1]\,gP(x)^{-1} = [x^2]\,P(x)^{-1} = x^{-1}x^2x^{-1} = 1.$$

By Lemma 5, $t \in I_H$. Now $g^{-1}g^\alpha = P(x)^{-1}\,t^{-1}t^\alpha P(x)^\alpha = P(x)^{-2}$. Suppose $g = u(P(y),\ u \in I_H,\ y \in H$. Then, similarly, $P(x)^{-2} = g^{-1}g^\alpha = P(y)^{-2}$; $P(x^2) = P(y^2)$; $x^2 = y^2$; $x = y$. Hence $u = gP(y)^{-1} = gP(x)^{-1} = t$.

(d) Let $g = tP(x)$, $t \in I_H$, $x \in H$. Since α fixes J, $P(x)^{-2} = g^{-1}g^\alpha \in J$. So $P(x)^2 \in J$. Since x has odd order, x is a power of x^2, and by Lemma 2, $P(x)$ is a power of $P(x)^2$. Therefore $P(x) \in J$, and $t = gP(x)^{-1} \in J$. The last equality is now obvious.

THEOREM 6. *Suppose* $\mathrm{Nuc}\,(H) = 1$.

(a) *There exists a unique automorphism ρ of M_H such that $P(x)^\rho = L(x)^{-1}$, $R(x)^\rho = P(x)^{-1}$, and $L(x)^\rho = R(x)$ for all $x \in H$.*

Take ρ as in (a).

(b) *If $P(x)^\rho = P(x)$, then $x^3 = 1$ and $L(x) = R(x)$.*

(c) *Also, $\alpha^{-1}\rho\alpha = \rho^2$, and ρ has order 3 if $H \neq 1$.*

(d) *If (U, V, W) is an autotopism of H and $U \in M_H$, then $V = U^\rho$ and $W = U^{\alpha\rho}$.*

(e) *If $U \in M_H$, then $(U, U^\rho, U^{\alpha\rho})$ is an autotopism of H.*

(f) *Suppose $U \in I_H$. Then $U^\rho = U$ if and only if U is an automorphism of H.*

Remark 3. By [2], p. 94, the elements x of H that satisfy $L(x) = R(x)$ form a commutative subloop H_0 of H. For such x, $T(x) = 1$, so by Lemma VII.2,2, p. 113, of [2], $x^3 \in \mathrm{Nuc}\,(H) = 1$. Thus H_0 is the set of elements x described in (b).

Proof. By Lemma 3, the autotopisms of H form a group. Suppose $A = (U, V, W)$ and $B = (U, V', W')$ are autotopisms of H with the same first member. Then $A^{-1}B = (1,\ V^{-1}V',\ W^{-1}W')$. By Lemma 3, $V^{-1}V' = W^{-1}W' = R(c)$ for some $c \in \mathrm{Nuc}\,(H)$. Since $\mathrm{Nuc}\,(H) = 1$, we have $R(c) = 1$ and $V = V'$, $W = W'$, and $A = B$. Thus V and W are uniquely determined by U. If $U \in M_H$ we let $V = U^\rho$. By Lemma 3, for every $x \in H$,

$A(x) = (P(x), L(x)^{-1}, L(x))$ and $B(x) = (R(x)^{-1}, P(x), R(x))$ are autotopisms of H. By Lemma 4(e), $M_K = R_K P_K = \langle R(x), P(x) : x \in H \rangle$. Since the autotopisms of H form a group, every element of M_K occurs as the first member, U, of some autotopism of H. Hence ρ is defined on M_H. Clearly, ρ is a homomorphism of M_H into itself.

Let $x \in H$. By considering $A(x)$ and $B(x)$ we see that $P(x)^\rho = L(x)^{-1}$ and $R(x)^\rho = P(x)^{-1}$. Hence $L(x)^\rho = (R(x)^{-1} P(x))^\rho = P(x) L(x)^{-1} = R(x)$. We see now that $\rho^3 = 1$. Hence ρ has an inverse, namely, ρ^2. Thus ρ is an automorphism of M_H. If σ is an automorphism of M_H and $P(x)^\sigma = L(x)^{-1} = P(x)^\rho$ and $R(x)^\sigma = P(x)^{-1} = R(x)^\rho$ for all $x \in H$, then $\sigma = \rho$ because $M_K = \langle R(x), P(x) : x \in H \rangle$. This proves (a).

By (a) and Lemma 6(a), $\alpha^{-1}\rho\alpha = \rho^2$. Let $x \in H$. If $P(x)^\rho = P(x)$, then

$$L(x)^{-1} = P(x), \qquad x^3 = [1]\, L(x)\, P(x) = 1,$$

and

$$R(x) = L(x)^{-1} P(x) = L(x)^{-2} = L(x^{-2}) = L(x).$$

If this holds for all $x \in H$, then H is commutative and hence centrally-nilpotent by the corollary to Theorem 4; since $Z(H) \subseteq \mathrm{Nuc}\,(H) = 1$, $H = 1$. Thus (b) and (c) are proved.

Let $x \in H$. Recall that

$$A(x) = (P(x), L(x)^{-1}, L(x)) \qquad \text{and} \qquad B(x) = (R(x)^{-1}, P(x), R(x)).$$

Now $P(x)^{\alpha\rho} = L(x)$ and $(R(x)^{-1})^{\alpha\rho} = R(x)$. From the first paragraph we now have (d) and (e).

Suppose $U \in I_H$. Then $U^\alpha = U$. If $U^\rho = U$, then $(U, U^\rho, U^{\alpha\rho}) = (U, U, U)$ is an autotopism of H. Thus for all $x, y, z \in H$, $([x]\, U)([y]\, U) = [xy]\, U$. Conversely, if U is an automorphism of H then (U, U, U) is an autotopism of H and $U = U^\rho = U^{\alpha\rho}$ from (d). Thus (f) holds and the proof is complete.

LEMMA 7. (a) *Let J be a subgroup of M_H and let $K = \{x \in H : P(x) \in J\}$. Then K is a subloop of $H(\frac{1}{2})$.*

Let J_1 be a normal subgroup of J and let $K_1 = \{x \in H : P(x) \in J_1\}$. Then K_1 is a normal subloop of K under $\circ$.

(b) *Let K be a subloop of $H(\frac{1}{2})$. Then K is a subloop of H if and only if $x^{-1}Kx = K$ for every $x \in K$.*

(c) *Suppose* $\mathrm{Nuc}\,(H) = 1$. *Take ρ as in Theorem 6. Let J be a subgroup of M_H fixed by α and ρ. Let $K = \{x \in H : P(x) \in J\}$. Then K is a subloop of H.*

Let J_1 be a normal subgroup of J fixed by α and ρ, and let $K_1 = \{x \in H : P(x) \in J_1\}$. Then K_1 is a normal subloop of K.

Proof. (a) K is a subloop of H by Lemma 2. Consider $P(K)$ with respect to $\circ'$ as defined in Lemma 2. The natural mapping of J onto J/J_1

takes $P(K)$ homomorphically onto a loop embedded in J/J_1. The kernel of this mapping is $J_1 \cap P(K)$, which equals $P(K_1)$. Hence $P(K_1)$ is a normal subloop of $P(K)$. By Lemma 2, K_1 is a normal subloop of K under $\circ$.

(b) Clearly, $x^{-1}Kx = K$ for all $x \in K$ if K is a subloop of H. Conversely, assume all these equalities hold. Suppose $x, y \in K$ and x has order $2n - 1$. Let $u = (x^{1(2)})^{-1}$. Then $u \in K$ and $x^{-1} \in K$, so K contains $u^{-1}(x \circ y)\, u = u^{-1}u^{-1}yu^{-1}u = u^{-2}y = xy$. Since H is di-associative, K is a subloop of H.

(c) By (a), K is a subloop of $H(\frac{1}{2})$. Let $x, y \in K$. Then $L(x)^{-1} = P(x)^{\rho} \in J$ and $R(x) = L(x)^{-1} P(x) \in J$. Hence $T(x) = L(x)^{-1} R(x) \in J$. Let $\sigma = T(x)$. Then J contains $\sigma^{-1}P(y)\, \sigma$. By Lemma 4(c), $\sigma^{-1}P(y)\, \sigma = P(y^{\sigma}) = P(x^{-1}yx)$. Hence $K \supseteq x^{-1}Kx$. Likewise, $K \supseteq xkx^{-1} \supseteq x(x^{-1}Kx)\, x^{-1} = K$. Thus $K = x^{-1}Kx$. Since x is arbitrary, K is a subloop of H by (b).

We see similarly that K_1 is a subloop of K. As in the above paragraph, we have $I_K \subseteq M_K \subseteq J$. Now I_K normalizes J_1. Hence by Lemma 4(d), I_K normalizes $P(H) \cap J = P(K_1)$. By Lemma 4(c), I_K fixes K_1. Thus every inner mapping of K fixes K_1, so K_1 is a normal subloop of K.

4. Solvable Normal Subloops

Theorem 7. *Let M be a minimal normal subloop of H. Suppose M is solvable. Then M is an elementary Abelian group and $(M, M, H) = 1$.*

Proof. We use induction on $|H|$. This is vacuously true if $H = 1$, so assume $|H| > 1$.

Since M is solvable, M has a proper normal subloop M_1 such that M/M_1 is a commutative group. Let p be a prime which divides $|M/M_1|$. Let $M_2 = \langle x^p : x \in M \rangle$. Clearly $M_2M_1/M_1 \neq M/M_1$, so M_2 is a proper subloop of M. Now let M_3 be the subloop of $M(\frac{1}{2})$ generated with respect to $\circ$ by the elements x^p, $x \in M$. Every automorphism of $M(\frac{1}{2})$ fixes M_3. In particular, by Lemmas 4(a) and 7(b), M_3 is a normal subloop of H. Since M is minimal and $M_3 \subseteq M_2 \neq M$, $M_3 = 1$. Thus $x^p = 1$ for all $x \in M$. By Theorem 1, $|M|$ is a power of p.

Suppose H contains a nonidentity normal subloop N that does not contain M. Since $M \cap N$ is normal in H but proper in M, $M \cap N = 1$. If N_1 is a normal subloop of H and $N \subseteq N_1 \subseteq NM$, then $N_1 = N(N_1 \cap M)$ and $N_1 \cap M$ is normal in H; thus $N_1 \cap M$ is 1 or M. Hence MN/N is a minimal normal subloop of H/N. By induction hypothesis, MN/N is an elementary Abelian group and $(MN/N, MN/N, H/N) = 1 = N/N$. Consequently, $(M, M, H) \subseteq (MN, MN, H) \subseteq N$. Also $M \cong MN/N$, which is an elementary Abelian group. Since M is a normal subloop of H, $(M, M, H) \subseteq M$; so $(M, M, H) \subseteq M \cap N = 1$.

Thus we may assume that every nonidentity normal subloop of H contains M. Suppose $\mathrm{Nuc}(H) \neq 1$. By Theorem VII.2.1, p. 114, and Lemma VII.3.2, p. 117, of [2], $\mathrm{Nuc}(H)$ is a normal subloop of H, and I_H induces a group of automorphisms of $\mathrm{Nuc}(H)$. Thus $\mathrm{Nuc}(H) \supseteq M$ and I_H induces a group of automorphisms of M, which is a group. Trivially, $(M, M, H) = 1$. Since $|M|$ is a power of p, $Z(M) \neq 1$. Now I_H fixes $Z(M)$; since M is a minimal normal subloop of H, $M = Z(M)$ and M is an elementary Abelian p-group.

Now we assume $\mathrm{Nuc}(H) = 1$. Let $M^* = \langle g^{-1}P_M g : g \in P(H)\rangle$. By Theorem 3, P_M is a p-group. By Theorem I.3, M^* is a normal subgroup of P_H, and $g^{-1}P_M g$ is a normal subgroup of M^* for each $g \in P(H)$. As a product of normal p-subgroups, M^* is a p-group. Since I_H fixes M, by Lemma 4(c) I_H normalizes $P(M)$ and therefore P_M. Hence by Lemma 4(d), I_H normalizes M^*. By Lemma 6, α fixes P_M, P_H, and therefore M^*. Let $J = \{x \in Z(M^*) : x^p = 1\}$. Then J is a nonidentity characteristic subgroup of M^*. Hence J is a normal subgroup of P_H which is fixed by α and normalized by I_H.

Assume $J \cap P(H) = 1$. Since α fixes J, by Lemma 6(d), $J \subseteq I_H$. Suppose $t \in J$ and $x \in H$. Let $y = x^{1/2}$. Then $P(y)\, tP(y)^{-1} \in J \subseteq I_H$. Hence $1 = [1]\, P(y)\, tP(y)^{-1}$, and $x = y^2 = [1]\, P(y) = [1]\, P(y)\, t = [x]\, t$. Thus $t = 1$. So $J = 1$, contrary to the above.

Hence $J \cap P(H) \neq 1$. Let $K = \{x \in H : P(x) \in J\}$. Since I_H normalizes J, by Lemma 7(b) K is a normal subloop of H. Hence $K \supseteq M$. Let $x, y \in M$. Recall that J is Abelian. Then $P(x)\, P(y) = P(y)\, P(x)$. Since $\mathrm{Nuc}(H) = 1$, we may apply ρ to this equation. By Theorem 6, we obtain $L(x)^{-1}\, L(y)^{-1} = L(y)^{-1}\, L(x)^{-1}$. Thus $L(y)\, L(x) = L(x)\, L(y)$. So

$$xy = [1]\, L(y)\, L(x) = [1]\, L(x)\, L(y) = yx.$$

Hence M is commutative. Since J is commutative, this yields

$$P(x)\, P(y) = P(x)^{1/2}\, P(y)\, P(x)^{1/2} = P(x \circ y) = P(x^{1/2} y x^{1/2}) = P(xy).$$

Applying ρ again, we have $L(y)\, L(x) = L(xy)$. For any $z \in H$, $x(yz) = (xy)\, z$. So $(M, M, H) = 1$. In particular, $(M, M, M) = 1$. Therefore M is a commutative group.

LEMMA 8. *Let p be a prime. Let A be a finite operator group on a nontrivial finite elementary p-group G. Suppose that p does not divide $|A|$. Then there exist subgroups $G_1, \ldots, G_n$ of G such that $G = G_1 \times \cdots \times G_n$ and, for each i, G_i is a subgroup of G which is minimal with respect to being fixed by A.*

Proof. We consider G as a vector space over the field of p elements. Then this is a special case of Maschke's theorem. ([8], Theorem 16.3.2, p. 255).

LEMMA 9 ([1], p. 71). *Let E be a nonempty subset of H, and let K be an associative subloop of H such that $(E, E, H) = (K, K, E) = 1$. Then E and K generate an associative subloop of H.*

LEMMA 10. *Let E be a normal subloop of H, and let K be a subloop of H such that $H = KE$. Then $H = K \circ E$, i.e., for each $h \in H$ there exist $k \in K$ and $j \in E$ such that $h = k \circ j$.*

Proof. Take $k \in K$ and $j' \in E$ such that $kj' = h$. In $H(\frac{1}{2})$ taken modulo E, $h \equiv k$, so $k^{-1} \circ h \equiv 1$. Let $j = k^{-1} \circ h$. Then $j \in E$ and

$$h = k \circ (k^{-1} \circ h) = k \circ j.$$

LEMMA 11. *Let A be a subgroup of the center of a group G. If G/A is cyclic, then G is commutative.*

Proof. Let $x \in G$ such that $\langle x, A \rangle = G$. Let $g_1, g_2 \in G$. There exist $a_1, a_2 \in A$ and integers i, j such that $g_1 = x^i a_1$, $g_2 = x^j a_2$. Then

$$g_1 g_2 = x^i a_1 x^j a_2 = x^i x^j a_1 a_2 = x^j x^i a_1 a_2 = x^j a_2 x^i a_1 = g_2 g_1 .$$

THEOREM 8. *Let K be an associative subloop of H. Let p be a prime. Then p divides $| M_K |$ if and only if p divides $| K |$.*

Remark 4. By using the Feit-Thompson theorem, one may obtain this result from Theorem 3.

Proof. Since the elements of M_K permute the elements of K transitively, $| K |$ divides $| M_K |$ ([8], p. 56). Thus if p divides $| K |$, then p divides $| M_K |$.

Suppose p does not divide $| K |$. Now $P_K \subseteq M_K$. Let

$$N = \{g \in M_K : [x]\, g = x \text{ for all } x \in K\}.$$

Since M_K fixes K, N is a normal subgroup of M_K. Now $M_K = \langle R(x), L(x) : x \in K \rangle$. Hence M_K/N is generated by the right and left translations of K, and $| M_K/N | = | K |\, s$, where s is the order of the inner automorphism group of K, i.e., $s = | K/Z(K) |$. Thus p does not divide $| M_K/N |$. Hence p does not divide $| P_K/P_K \cap N |$. Let Q be a Sylow p-subgroup of P_K; then $Q \subseteq P_K \cap N$.

Let $\sigma \in Q$ and let $x \in K$. Since $\sigma \in N$, $[1]\, \sigma = 1$. By Lemma 5, $\sigma \in I_K$. Likewise, $[x]\, \sigma = x$. By Lemma 4(c), $\sigma^{-1} P(x)\, \sigma = P(x^\sigma) = P(x)$. Since x is arbitrary, $\sigma \in Z(P_K)$. Thus $Q \subseteq Z(P_K)$. So Q is in the center of its normalizer in P_K. By a theorem of Burnside ([8], Theorem 14.3.1, p. 203), P_K has a normal subgroup R of index $| Q |$ in P_K. Let $x \in K$. Then $P(x)$ has order prime to $| Q |$. Hence $P(x) \equiv 1$, modulo R; $P(x) \in R$. So $P_K \subseteq R$ and $Q = 1$.

Thus p does not divide $|P_K|$. As in the proof of Theorem 3, we see that p does not divide $|L_K|$. By Lemma 4(e), p does not divide $|M_K|$.

THEOREM 9. *Let E and K be subloops of H such that $(E, E, H) = 1$ and I_K normalizes E. Then KE is a subloop of H and E is a normal subloop of KE.*

Proof. To show that KE is a subloop of H it suffices to show that KE is closed with respect to multiplication. Let $u, v \in K$ and $a, b \in E$. Let $w = vu^{-1}$. Then $ua = ([a]\, T(u^{-1}))\, u \in EK$. Thus for suitable elements $\sigma_1, \ldots, \sigma_5$ of I_K we have

$$(ua)(vb) = (ua)(b^{\sigma_1}v) = (ua)((b^{\sigma_2}w)\, u) = u(a(b^{\sigma_2}w))\, u = u((ab^{\sigma_2})\, w)\, u$$

$$= u(((ab^{\sigma_2})\, w)\, u) = u((ab^{\sigma_2})^{\sigma_3}\, v) = u(v(ab^{\sigma_2})^{\sigma_4}) = (uv)\,(ab^{\sigma_2})^{\sigma_5}.$$

Thus KE is a loop and $(uE)(vE) = (uv)\, E$. It is now easy to see that the mapping $x \to xE$ is a homomorphism of KE with kernel E. Hence E is a normal subloop of KE.

THEOREM 10. *Let E be a normal subloop of H. Suppose that:*

(a) *E is a solvable loop:*

(b) *$|E|$ and $|H/E|$ are relatively prime; and*

(c) $(E, E, H) = 1$.

Then $E \subseteq \mathrm{Nuc}\,(H)$.

Remark 5. By (c), E is associative. Hence (a) follows from (c) and the Feit-Thompson theorem.

Proof. Assume the theorem is false. Let H be a counterexample of minimal order. By Theorem VII.2.1, p. 114, of [2], there exist $x_1, y_1 \in H$ and $z_1 \in E$ such that $(x_1, y_1, z_1) \neq 1$. Let $H_1 = \langle x_1, y_1, z_1\rangle$. Then $H_1/H_1 \cap E \cong H_1E/E \subseteq H/E$. By Theorem 2, $|H_1/H_1 \cap E|$ divides $|H/E|$ and $|H_1 \cap E|$ divides $|E|$. Hence H_1 satisfies the hypothesis. Since $(x_1, y_1, z_1) \neq 1$, $H_1 = H$.

Let $K_1 = \langle x_1, y_1\rangle$. Then $H = \langle K_1, E\rangle = K_1E$. Thus $K_1/K_1 \cap E \cong H/E$. In particular, $|K_1/K_1 \cap E|$ is relatively prime to $|K_1 \cap E|$. Since K_1 is a group, Theorem 15.2.2, p. 244 of [8] asserts that K_1 contains a subgroup K such that $K_1 = K(K_1 \cap E)$ and $K \cap E = 1$. Then

$$H = \langle K_1, E\rangle = \langle K, K_1 \cap E, E\rangle = \langle K, E\rangle = KE$$

and $|K| = |K/K \cap E| = |KE/E| = |H/E|$. Since K is a group, by Theorem 8 $|M_K|$ is relatively prime to $|E|$.

If $(K, K, E) = 1$, then by Lemma 9 $H = \langle K, E\rangle$ is associative, contrary to

hypothesis. Let $x, y \in K$ and $z \in E$ such that $(x, y, z) \neq 1$. Let $\sigma = L(y)L(x)L(xy)^{-1}$. Let E_1 be a minimal normal subloop of H contained in E. By Theorem 7, E_1 is an elementary Abelian p-group for some prime p. Suppose $E_1 \neq E$. Then $\langle K, E_1 \rangle = KE_1 \neq H$. By induction hypothesis, σ centralizes E_1 and E/E_1. Let $z^\sigma = w \circ z$. Since σ centralizes E/E_1, $w \in E_1$. By Lemma 4(a), $z^{\sigma^2} = (z^\sigma)^\sigma = (w \circ z)^\sigma = w^\sigma \circ z^\sigma = w \circ (w \circ z) = w^2 \circ z$. By induction we find that $z^{\sigma^p} = w^p \circ z = 1 \circ z = z$. So σ^p fixes z. Since the order of M_K is prime to p, σ fixes z, contrary to hypothesis. So $E_1 = E$.

Thus E is an elementary Abelian p-group. Suppose $x, y \in E$ and $\tau \in I_K$. Let $u = x^{1/2}$. By Lemma 4(a), $(xy)^\tau = (u^2y)^\tau = (uyu)^\tau = u^\tau y^\tau u^\tau = (u^\tau)^2 y^\tau = (u^2)^\tau y^\tau = x^\tau y^\tau$. So I_K induces a group of automorphisms on E. By Lemma 8, there exist subgroups $E_1, \ldots, E_n$ of E such that $E = E_1 \times \cdots \times E_n$ and each E_i is minimal with respect to being fixed by I_K. Take σ as in the above paragraph. There exists i such that σ does not centralize E_i. By Theorem 9, KE_i is a loop. Clearly E_i and KE_i satisfy the hypothesis of the theorem. Since σ is nontrivial on E_i, $KE_i = H$ and $E = E_i$. Thus E is a minimal normal subloop of H. As in the third paragraph of the proof of Theorem 7, we see by induction hypothesis that every nontrivial normal subloop of H contains E. Hence Nuc $(H) = 1$.

Now let L be any proper subgroup of K. Then $\langle L, E \rangle = LE$, and LE is a proper subloop of H. By induction hypothesis, $E \subseteq$ Nuc (LE). Hence, by Lemma 9, LE is associative. Let $x, y \in L$. Let $\sigma = R(x)R(y)R(xy)^{-1}$. Then σ fixes every element of LE. Likewise, σ fixes every element of K. By Lemma 4(b) the elements of H fixed by σ form a subloop of H. By Lemma 10, this subloop is H. Thus $\sigma = 1$. But σ has companion $x^{-1}y^{-1}xy$ ([2], Lemma VII. 2.2, p. 113), so $x^{-1}y^{-1}xy \in$ Nuc $(H) = 1$. Hence $xy = yx$. Since x and y are arbitrary, L is commutative; that is, every proper subgroup of K is commutative.

Let J_1 be any associative subloop of H such that $J_1E = H$. As we saw for K_1 above, J_1 contains a subgroup J such that $JE = H$, $J \cap E = 1$, and I_J fixes no proper subgroup of E except 1. But I_J fixes $J_1 \cap E$. If $J_1 \cap E = E$ then $J_1 = H$. Hence $J_1 \cap E = 1$.

Suppose K is commutative. From the above, $K = \langle x, y \rangle$ for some x and some y. Let $z \in E$ and let $J = \langle x, y \circ z \rangle$. Then J is associative and $H = \langle x, y, E \rangle = \langle x, y \circ z, E \rangle = \langle J, E \rangle = JE$. By the above paragraph, $J \cap E = 1$. Hence $J \cong H/E \cong K$, and J is commutative. So $T(x)$ fixes $y \circ z$. By Lemma 4(b), the elements of H fixed by σ form a subloop of $H(\frac{1}{2})$. Since $T(x)$ fixes y, $T(x)$ fixes $y^{-1} \circ (y \circ z) = z$. Thus $T(x)$ fixes every element of K and of E. By Lemma 10, $T(x) = 1$. Now suppose $z \in E$ and $z \neq 1$. Since x and z commute and have relatively prime orders, x and z are both powers of xz. Let $J_1 = \langle xz, y \rangle$. Then

$$J_1E = \langle J_1, E \rangle = \langle xz, y, E \rangle = \langle x, y, E \rangle = H,$$

and J_1 is associative. By the above paragraph, $J_1 \cap E = 1$. But $z \in \langle xz \rangle \subseteq J_1$, a contradiction. Thus K is not commutative.

Let $Z = Z(K)$. Since K is not commutative, Z is a proper subgroup of K. Hence $\langle Z, E \rangle = ZE$ is a proper subloop of H. By induction hypothesis, $E \subseteq \mathrm{Nuc}\,(ZE)$. By Lemma 9, ZE is associative. Let $x \in Z$, $y \in E$, and let $\sigma = R(x)\,R(y)\,R(xy)^{-1}$. Then σ fixes every element of E. Let $w \in K$. By Lemma 11, $\langle Z, w \rangle$ is a proper subgroup of K. Hence $\langle Z, w, E \rangle$ is a proper subloop of H. As with ZE above, σ fixes w. So σ fixes every element of K and of E. By Lemmas 4(b) and 10, $\sigma = 1$. But σ has companion $x^{-1}y^{-1}xy$. Hence $x^{-1}y^{-1}xy \in \mathrm{Nuc}\,(H) = 1$, and $xy = yx$. So Z centralizes E. Since Z is commutative, it is contained in the center of ZE. It is easy to see that Z consists of all the elements of ZE which have order prime to p. Since ZE is a normal subloop of H, I_H fixes Z by Lemma 4(a). We saw above that every nontrivial normal subloop of H contains E; hence $Z = 1$.

Let L be any nontrivial Sylow subgroup of K. Since $Z(L) \neq 1$, $L \neq K$. Hence L is commutative, $\langle L, E \rangle = LE$, and LE is a group. Suppose L is not cyclic. Let L_1 be an elementary subgroup of L of order p^2. Now, every nonidentity element of L_1 is contained in a unique subgroup of order p. By a result of Wielandt ((3.3), p. 149, of [*10*]), some nonidentity element u of L_1 centralizes some nonidentity element v of E. Since $Z(K) = 1$, we may take $w \in K$ such that $\langle u, w \rangle$ is non-Abelian. Hence $\langle u, w \rangle = K$. Now let $J = \langle uv, w \rangle$. Then $JE = \langle J, E \rangle = \langle uv, w, E \rangle = \langle u, w, E \rangle = KE = H$. By one of the above paragraphs, $J \cap E = 1$. But $v \in \langle uv \rangle$, because $uv = vu$ and u and v have relatively prime orders. So $v \in J \cap E$. This contradiction shows that every Sylow subgroup of L is cyclic.

Let q be the largest prime divisor of $| K |$, and let Q be a Sylow q-subgroup of K. Since every Sylow subgroup of K is cyclic, Q is a normal subgroup of K by a well-known theorem ([*3*], p. 163-164). Let Q_1 be the unique subgroup of order q in Q. Then Q_1 is a characteristic subgroup of Q and hence a normal subgroup of K. Since $Z(K) = 1$ there exists $z_1 \in K$ such that z_1 does not centralize Q. Since $\langle z_1, Q \rangle$ is non-Abelian, $\langle z_1, Q_1 \rangle = K$. Let z be some power of z_1 that has prime order, say, r. If z centralizes Q_1, then $z \in Z(\langle z_1, Q_1 \rangle) = Z(K) = 1$, a contradiction. So z does not centralize Q_1. Hence $K = \langle z, Q_1 \rangle$, $r \neq q$, $Q_1 = Q$, and $| K | = qr$. Let $R = \langle z \rangle$.

Let us consider the inner mapping $T(z)$. By the above, r divides $q - 1$ and there exists an integer i such that $i \not\equiv 1$, modulo q, and $z^{-1}yz = y^i$ for all $y \in Q$. Also $\langle R, E \rangle = RE$ is a proper subloop of H. Hence by induction hypothesis and Lemma 9, RE is associative. Thus $T(z)$ induces an automorphism on E. Let us take any $y \in QE$ such that $y \notin E$. Let $J = \langle z, y \rangle$. Clearly $\langle y, E \rangle = QE$ and so $JE = \langle J, E \rangle = \langle z, QE \rangle = H$. By an above paragraph, $J \cap E = 1$. Hence $J \cong J/J \cap E \cong JE/E = H/E$. Thus $z^{-1}yz = y^i$.

Now let y be an arbitrary nonidentity element of Q. As QE is a group, $T(y)$ induces an automorphism on E. Let E_1 be a subgroup of E that is minimal with respect to being fixed by $T(y)$. By the methods used above, we see that no element of E is fixed by $T(y)$ or $T(z)$ except the identity element. Let γ be the automorphism of E_1 induced by $T(y)$. Then $\gamma \neq 1$. By Schur's lemma ([8], Theorem 16.6.2, p. 269), the subring F of the ring of endomorphisms of E_1 generated by γ is a field. Note that $\langle Q, E_1 \rangle = QE_1$.

Let $x \in E_1$. Then $yxy \in QE_1$, but $yxy \notin E_1$. By the above,

$$(yxy)^i = (yxy)^{T(z)} = y^{T(z)}x^{T(z)}y^{T(z)} = y^i x^{T(z)} y^i.$$

Thus $x^{T(z)} = y^{-i}(yxy)^i y^{-i} \in E \cap QE_1 = E_1$; therefore, $T(z)$ induces an automorphism β on E_1. Now

$$y^i x^\beta y^i = y^{2i} y^{-i} x^\beta y^i = y^{2i} x^{\beta\gamma^i}.$$

An easy induction argument shows that

$$(yxy)^i = (y^2 x^\gamma)^i = y^{2i}(x^\gamma)^{\gamma^{2i-2}}(x^\gamma)^{\gamma^{2i-4}} \cdots (x^\gamma)^2 (x^\gamma).$$

Hence

$$\beta = \gamma^{-i}\gamma(\gamma^{2i-2} + \gamma^{2i-4} + \cdots + \gamma^2 + 1).$$

Thus we even have $\beta \in F$.

Similarly,

$$(xy^2x)^i = (xy^2x)^{T(z)} = x^\beta y^{2i} x^\beta = y^{2i}(x^\beta)^{\gamma^{2i}} x^\beta,$$

and

$$(xy^2x)^i = (y^2 x x^{\gamma^2})^i = y^{2i}(x x^{\gamma^2})^{(\gamma^{2i-2}+\cdots+\gamma^2+1)}.$$

Hence

$$(1 + \gamma^2)(\gamma^{2i-2} + \cdots + \gamma^2 + 1) = \beta(1 + \gamma^{2i}).$$

Since y has odd order, $\gamma^4 \neq 1$, so $\gamma^2 \neq -1$. Therefore, $1 + \gamma^2$ is invertible, and $\gamma^{2i-2} + \cdots + \gamma^2 + 1 = \beta(1 + \gamma^{2i})(1 + \gamma^2)^{-1}$. By the above paragraph, $\beta(1 + \gamma^{2i})(1 + \gamma^2)^{-1} = \beta\gamma^{i-1}$. Since β is invertible, $(1 + \gamma^{2i})(1 + \gamma^2)^{-1} = \gamma^{i-1}$, and

$$\gamma^{-i}(1 + \gamma^{2i}) = (1 + \gamma^2)\gamma^{-1} = \gamma^i + \gamma^{-i} = \gamma + \gamma^{-1}.$$

Let $\gamma_1 = \gamma + \gamma^{-1}$. If $t \in F$ and $t + t^{-1} = \gamma_1$, then $t^2 - \gamma_1 t + 1 = 0$. Since F is a field, there are at most two solutions for t in the equation. But γ, γ^{-1}, γ^i, and γ^{-i} are solutions. Since y has odd order, $\gamma \neq \gamma^{-1}$. By assumption, $y^i \neq y$, so $\gamma^i \neq \gamma$. Hence

$$\gamma^i = \gamma^{-1}, \qquad y^i = y^{-1}, \qquad x^{-2}yx^2 = y^{i^2} = (y^i)^{-1} = (y^{-1})^{-1} = y.$$

So x^2 centralizes y. Since x has odd order, x centralizes y, contrary to the above. This contradiction completes the proof of the theorem.

COROLLARY. *Let E be a minimal normal subloop of H. Suppose $|E|$ and $|H/E|$ are relatively prime and E is solvable. Then $E \subseteq \mathrm{Nuc}(H)$.*

5. HALL AND SYLOW THEOREMS

Let π be a set of primes. For each positive integer n we let n_π be the largest π-number that divides n. We say that a subloop K of H is a *Hall π-subloop* of H if $|K| = |H|_\pi$. If π contains only one prime p, we also call a Hall π-subloop a *Sylow p-subloop*. Recall that by Theorem 1 a subloop K of H is a π-subloop of H if and only if $|K|$ is a π-number.

THEOREM 11. *Suppose H is a solvable loop. Let π be a set of primes. Then every Hall π-subloop of $H(\frac{1}{2})$ is a Hall π-subloop of H.*

Proof. We use induction on $|H|$. The result is trivial if $H = 1$. Assume $|H| > 1$.

Let K be a Hall π-subloop of $H(\frac{1}{2})$. Then $|K| = |H|_\pi$. We must show that K is a subloop of H. Since H is finite, it is sufficient to show that K is closed with respect to multiplication.

Let M be a minimal normal subloop of H. By Theorem 7, M is an elementary p-group for some prime p, and $(M, M, H) = 1$. It is easy to see that KM/M is a Hall π-subloop of $(H/M)(\frac{1}{2})$. Hence by induction hypothesis KM is a subloop of H. Since K is a Hall π-subloop of $KM(\frac{1}{2})$, we may assume that $KM = H$. If $p \in \pi$, then $H = K$. Hence we may assume $p \notin \pi$. By Theorem 10, $M \subseteq \mathrm{Nuc}(H)$.

Now let x and y be arbitrary elements of K and let $L = \langle x, y, M \rangle$. Since K contains exactly one element from each coset of M in H, $|K \cap L| = |L/M| = |L|_\pi$. By induction hypothesis $xy \in K \cap L \subseteq K$, except possibly if $L = H$. Let us assume $L = H$. By Lemma 9, H is a group because $\langle x, y \rangle$ is associative and $M \subseteq \mathrm{Nuc}(H)$. By Theorem I.6(iii), K generates a π-subgroup K_0 of H. Since $|H|_\pi = |K| \leqslant |K_0| \leqslant |H|_\pi$, $K = K_0$. So $xy \in K$. Since x and y are arbitrary, K is a Hall π-subloop of H.

THEOREM 12. *Suppose H is a solvable loop. Let π be a set of primes. Then:*

(a) *H contains a Hall π-subloop.*

(b) *The Hall π-subloops of H are transitively-permuted by $P_H \cap I_H$. Every prime which divides the number of Hall π-subloops of H also divides $|H|$ and lies outside π.*

(c) *Every π-subloop of H is contained in a Hall π-subloop of H.*

Proof. By Theorem 3, $H(\frac{1}{2})$ is a solvable loop. Hence by Theorem I.8, $H(\frac{1}{2})$ satisfies (a) and (c), and the Hall π-subloops of $H(\frac{1}{2})$ are permuted transitively by the group T_H as defined on page 382 of I. It is not difficult to verify that the group T_H coincides with $P_H \cap I_H$. Hence all parts of this theorem follow from Theorem 11.

LEMMA 12. *Let J be a subloop of $H(\frac{1}{2})$. Suppose J contains a (Moufang) subloop K of H such that:*

(a) *with respect to $\circ$, K is a normal subloop of J;*

(b) *with respect to $\circ$, J is generated by K and some element z of J; and*

(c) *each element of I_K maps J onto itself.*

Then J is a subloop of H.

Proof. Let $n = |J|/|K|$. Suppose $x \in K$ and $1 \leqslant i \leqslant n$. Then $x \circ z^i \in J$. Let $u = x^{1/2}$. Since $T(u) \in I_K$, J contains

$$[x \circ z^i]\ T(u) = [uz^iu]\ T(u) = u^{-1}(uz^iu)\, u = z^iu^2 = z^ix.$$

Thus J contains the set $J_1 = \{z^ix : 1 \leqslant i \leqslant n, x \in K\}$.

Now suppose $x, y \in K$, $1 \leqslant i, j \leqslant n$, and $z^ix = z^jy$. We may assume $i \leqslant j$. Then $x = z^{-i}(z^ix) = z^{-i}(z^jy) = z^{j-i}y$, and $z^{j-i} = xy^{-1} \in K$. Under $\circ$, $\langle z\rangle/(\langle z\rangle \cap K) \cong \langle z, K\rangle/K = J/K$. Hence $\langle z\rangle/(\langle z\rangle \cap K)$ has order n. Since $0 \leqslant j - i \leqslant n - 1$, $i = j$. Thus $z^i = z^j$ and $x = y$. Thus $|J_1| = n|K| = (|J|/|K|)|K| = |J|$. So $J = J_1$. Taking inverses, we obtain $J = \{xz^i : x \in K, 1 \leqslant i \leqslant n\}$.

Let $a, b \in J$. There exist $x, y \in K$ and integers i, j such that $a = z^ix$ and $b = yz^j$. By [2], VII(3.1), p. 115.

$$\begin{aligned} z^{-2i} \circ ab &= z^{-i}(ab)\, z^{-i} = (z^{-i}a)\,(bz^{-i}) = x(yz^{j-i}) \\ &= [(xy)\, z^{j-i}]\, L(xy)^{-1} L(y) L(x). \end{aligned}$$

By condition (c), $z^{-2i} \circ ab \in J$. Hence $ab = z^{2i} \circ (z^{-2i} \circ ab) \in z^{2i} \circ J = J$. Thus J is a subloop of H.

THEOREM 13. *Let p be a prime, and let K be a p-subloop of H. Then K is contained in some Sylow p-subloop of H.*

Proof. Let $|H|_p$ be the highest power of p which divides $|H|$. By Theorems 1 and 2, $|K|$ is a power of p and $|K|$ divides $|H|$. Hence $|K|$ divides $|H|_p$. We use induction on $|H|_p/|K|$. The statement is trivial if $|H|_p/|K| = 1$. Hence we may assume $|H|_p > |K|$.

By Theorem 4, K is centrally nilpotent. Hence, by Theorem 3, M_K is a p-group. We see from Lemmas 4(d) and 6 that P_K is a normal subgroup of M_K and that α fixes both P_K and M_K.

Let $L = \{g \in M_H : [K]g = K\}$. Then $M_K \subseteq L$. Let R be a Sylow p-subgroup of L that contains M_K. Suppose $g \in R$ and $y = [1]g$; then $y \in K$. By Lemma 6, $g^{-1}g^{\alpha} = P(y)^{-1} \in P_K \subseteq R$. Hence $g^{\alpha} \in gR = R$. Since g is arbitrary, $R^{\alpha} \subseteq R$, so $R = R^{\alpha^2} \subseteq R^{\alpha}$. Thus α fixes R. By Lemma 6(d), $|R| = |R \cap I_H|\,|R \cap P(H)| = |R \cap I_H|\,|K|$ and $|M_H| = |I_H|\,|H|$. Since $|R \cap I_H|$ divides $|I_H|$, and since $|K|$ properly divides $|H|_p$, p divides $[M_H : R]$. Let N be the normalizer of R in M_H. By Sylow's Theorem, p divides $[N : R]$.

Clearly, α fixes N. Let $K_0 = \{x \in H : P(x) \in N\}$. By Lemma 7(a), K and K_0 are subloops of $H(\frac{1}{2})$ and K is a normal subloop of K_0. By Lemma 6,

$$|N| = |N \cap I_H|\,|N \cap P(H)| = |N \cap I_H|\,|K_0|.$$

Hence

$$[N : R] = [N \cap I_H : R \cap I_H]\left|\frac{K_0}{K}\right|.$$

Suppose p divides $[N \cap I_H : R \cap I_H]$. Suppose $\sigma \in N \cap I_H$ and $\sigma \notin R \cap I_H$ but $\sigma^p \in R \cap I_H$. Now, σ normalizes R. By Lemma 4(d), σ normalizes $R \cap P(H)$, which equals $P(K)$. By Lemma 4(c), $[K]\sigma = K$. But then $\langle R, \sigma\rangle$ is a p-subgroup of L that properly contains R. This is impossible because R is a Sylow p-subgroup of L. Hence p does not divide $[N \cap I_H : R \cap I_H]$. Since p divides $[N : R]$, p must divide $|K_0/K|$. By Corollary 1 of Theorem I.9, K_0/K contains a cyclic subloop $\bar{J}$ of order p. Let J be the subloop of K_0 such that $J \supseteq K$ and $J/K = \bar{J}$. Let $z \in J$ such that $z \notin K$. Let $S = \langle R, P(z)\rangle$. Since $P(z) \notin R$ but $P(z)^p = P(z^p) \in P(K) \subseteq R$, $|S/R| = p$. By Lemma 6(d),

$$p = \left|\frac{S}{R}\right| = [S \cap I_H : R \cap I_H]\left|\frac{S \cap P(H)}{R \cap P(H)}\right|.$$

But $|S \cap P(H)/R \cap P(H)| \geqslant |P(J)/P(K)| = |J/K| = p$. Hence $S \cap P(H) = P(J)$. By Lemma 4(d), I_K normalizes $P(J)$; by Lemma 4(c), I_K fixes J. By Lemma 12, J is a subloop of H. Since $|H|_p/|J| < |H|_p/|K|$, by induction hypothesis J is contained in some Sylow p-subloop H_p of H. Since $K \subseteq J \subseteq H_p$, the proof is complete.

Taking $K = 1$ in Theorem 13, we obtain:

COROLLARY. *Let p be a prime. Then H contains at least one Sylow p-subloop.*

6. Solvability of Certain Finite Loops

As in I, we define a *B-loop* to be a power-associative loop which satisfies (1) and which consists of elements of finite odd order. We use the notation of I throughout this section.

THEOREM 14. *Let K be a finite B-loop. Then:*

(a) *the canonical group G_K has odd order; and*

(b) *K is solvable.*

Proof. (a) Let M be the group of permutations of K generated by G_K and a_K. By Theorem I.2(v), a_K normalizes G_K, and $g^{-1}(a_K)^{-1}ga_K$ has odd order for all $g \in G_K$. Hence $M = \langle G_K, a_K \rangle$, and $g^{-1}(a_K)^{-1}ga_K$ has odd order for all $g \in M$. Since $[x]\, a_K = x^{-1}$ for all $x \in K$, $(a_K)^2 = 1$. Now, by Theorem 1 of [6], there exists in M a normal subgroup N of odd order such that $a_K N$ lies in the center of M/N. By Theorem I.2(v) and the definition of G_K, the elements of the form $g^{-1}(a_K)^{-1}ga_K$ for $g \in G_K$ form a set of generators of G_K. Hence $G_K \subseteq N$.

(b) By (a) and by Corollary 2 of Theorem I.6, K is solvable.

Remark 6. Corollary 2 of Theorem I.6 is the only result in I that depends on the Feit-Thompson theorem. Thus Theorem 14(a) and the preceding results of this paper do not require the Feit-Thompson theorem.

COROLLARY 1. *Let H be a finite B-loop half-embedded in a group G. Let π be the set of all prime divisors of $|H|$. Then H^* is a finite solvable π-subgroup of G, and, for each prime p in π, there exists an element of order p in H. In particular, H^* has odd order.*

Proof. By Theorem I.1(iv), H^* is finite. Moreover, by Theorem 14 and Theorem I.6(ii), H^* is solvable. By Proposition I.1, $|H|$ is odd. Therefore, π contains only odd primes. The remainder of the corollary follows from Theorem I.6(iii) and Corollary 2 of Theorem I.9.

COROLLARY 2. *Let H be a finite B-loop. There exists a finite group G of odd order and an automorphism α of G such that:*

(a) *H is half-embedded in G;*

(b) *H generates G; and*

(c) *H is the set of all elements of the form $g^{-1}g^{\alpha}$ for $g \in G$.*

Proof. By Theorem I.2 and Theorem 14, we may take G to be isomorphic to G_H.

THEOREM 15. *Let H be a finite non-empty subset of a group. Suppose that*

(a) *every element of H has finite odd order; and*

(b) *whenever $x, y \in H$, then $xyx \in H$.*

Let π be the set of all prime divisors of $|H|$. Then H generates a finite solvable

π-subgroup of G, and, for each prime p in π, there exists an element of order p in H. In particular, H generates a subgroup of G that has odd order.

Proof. By Corollary 1 of Theorem 14, we need only show that H forms a B-loop that is half-embedded in G. By Lemma I.3, this is true if $x^{1/2} \in H$ for every $x \in H$. Suppose $x \in H$ and x has order $2n - 1$. If n is even, let $m = 3n - 1$. If n is odd, let $m = n$. Then m is odd and $x^m = x^n = x^{1/2}$. Now, $x^1 = x \in H$. Also, whenever $x^i \in H$ then $x^{i+2} = xx^ix \in H$. Thus $x^i \in H$ for every odd integer i. Hence $x^{1/2} \in H$.

Remark 7. The proof of Theorem 15 actually shows that the assumption that $x^{1/2} \in H$ for every $x \in H$ is superfluous in Lemma I.3. It is possible to prove Theorem 15 by using only group-theoretical means.

THEOREM 16. *Every finite Moufang loop of odd order is solvable.*

Proof. Assume H is an arbitrary finite simple Moufang loop of odd order. It is sufficient to prove that H is an Abelian group. By Theorem 14(b), $H(\frac{1}{2})$ is solvable. Let N be the commutator-associator subloop of $H(\frac{1}{2})$ ([2], p. 13). Then N is a proper subloop of $H(\frac{1}{2})$ that is fixed by every automorphism of $H(\frac{1}{2})$. By Lemma 4(a), every inner mapping of H fixes N. By Lemma 7(b), N is a subloop, and therefore a normal subloop, of H. Since H is simple, $N = 1$. Thus $H(\frac{1}{2})$ is an Abelian group. Let p be a prime divisor of $|H|$, and let N_p be the subgroup of $H(\frac{1}{2})$ that consists of the elements $x \in H$ that satisfy $x^p = 1$. Then N_p, like N, is fixed by every automorphism of $H(\frac{1}{2})$ and is therefore a normal subloop of H. Since $N_p \neq 1$, $N_p = H$. By Theo- 1 and 4, $Z(H) \neq 1$. Hence $Z(H) = H$; i.e., H is an Abelian group.

ACKNOWLEDGMENT

I would like to thank the National Science Foundation for its partial support during the preparation of this paper.

REFERENCES

1. BRUCK, R. H. Pseudo-automorphisms and Moufang loops. *Proc. Am. Math. Soc.* 3 (1952), 66-72.
2. BRUCK, R. H. "A Survey of Binary Systems." Springer, Berlin, 1958.
3. BURNSIDE, W. "Theory of Groups of Finite Order." Cambridge Univ. Press, Cambridge, 1911.
4. FEIT, W. AND THOMPSON, J. G. Solvability of groups of odd order. *Pacific J. Math.* 13 (1963), 775-1029.
5. GLAUBERMAN, G. On loops of odd order. *J. Algebra* 1 (1964), 374-396.
6. GLAUBERMAN, G. Central elements in core-free groups. *J. Algebra* 4 (1966), 403-420.

7. GLAUBERMAN, G. AND WRIGHT, C. R. B. Nilpotence of finite Moufang 2-loops. *J. Algebra* **8** (1968), 415-417.
8. HALL, M. "The Theory of Groups." Macmillan, New York, 1959.
9. PAIGE, L. J. A class of simple Moufang loops. *Proc. Am. Math. Soc.* **7** (1956), 471-482.
10. WIELANDT, H. Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppen einer endlichen Gruppe. *Math. Z.* **73** (1960), 146-158.